Claims

1. A validation protocol for determining whether an untrusted authentication chip is valid, or not, including the steps of:

generating a secret random number and calculating a signature for the random number using a signature function, in a trusted authentication chip;

encrypting the random number and the signature by a symmetric encryption function using a first key, in the trusted authentication chip;

passing the encrypted random number and signature from the trusted authentication chip to an untrusted authentication chip;

decrypting the encrypted random number and signature with a symmetric decryption function using the first key, in the untrusted authentication chip;

calculating a signature for the decrypted random number using the signature function, in the untrusted authentication chip;

comparing the signature calculated in the untrusted authentication chip with the signature decrypted;

in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using a second key and returning it to the trusted authentication chip;

encrypting the random number by the symmetric encryption function using the second key, in the trusted authentication chip;

comparing the two random numbers encrypted using the second key, in the trusted authentication chip;

in the event that the two random numbers encrypted using the second key match, considering the untrusted authentication chip to be valid;

otherwise considering the untrusted authentication chip to be invalid.

2. The protocol according to claim 1, where the first and second keys are held in both the trusted and untrusted authentication chips, and are kept secret.

3. The protocol according to claim 1, where the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after each successful validation, so that the next random number will be produced from a new seed.

4. The protocol according to claim 1, where the symmetric decrypt function is held only in the untrusted chip.

5. The protocol according to claim 1, where the signature function generates digital signatures of 160 bits.

6. The protocol according to claim 1, where a prove function is held only in the untrusted chip to test the decrypted random number and signature, and return the random number encrypted with the second key if a signature calculated from the decrypted random number matches the decrypted signature; otherwise it returns an indication the chip is invalid.

7. The protocol according to claim 6, where the time taken to return an indication the chip is invalid is the same for all bad inputs, and the time taken to return the random number encrypted with the second key is the same for all good inputs.

8. The protocol according to claim 1, where a test function is held only in the trusted chip to advance the random number if the untrusted chip is valid; otherwise it returns an indication the chip is invalid.

9. The protocol according to claim 8, where the time taken to return an indication the chip is invalid is the same for all bad inputs, and the time taken to return an indication the chip is valid is the same for all good inputs.

10. The protocol according to claim 1, where it is used to determine the physical presence of a valid authentication chip.

11. A validation system for performing the method according to claim 1, where the system includes a trusted authentication chip and an untrusted authentication chip; where the trusted authentication chip includes a random number generator, a symmetric encryption function and two keys for the function, a signature function and a test function; and the untrusted authentication chip includes a symmetric encryption and decryption function and two keys for these functions, a signature function, and a prove function to decrypt a random number and signature encrypted using the first key by the trusted authentication chip, and to calculate another signature from the decrypted random number, for comparison with the decrypted one, and in the event that the comparison is successful to encrypt the random number with the second key and send it back; the test function in the

trusted chip then operates to generate an encrypted version of the random number using the second key and to compare it with the received version to validate the untrusted chip.

12. A validation system according to claim 11, where the remainder of the system is software, hardware or a combination of both, but the trusted chip is a physical authentication chip.

13. A validation system according to claim 11, where both chips have the same internal structure.

14. A validation system according to claim 11, where the first and second keys are kept secret.

15. A validation system according to claim 11, where the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after each successful validation, so that the next random number will be produced from a new seed.

16. A validation system according to claim 11, where the signature function generates digital signatures of 160 bits.

17. A validation system according to claim 11, where the prove function returns an indication the chip is invalid for all bad inputs and the time taken to do this is the same for all bad inputs, and the time taken to return the random number encrypted with the second key is the same for all good inputs.

18. A validation system according to claim 11, where the test function advances the random number if the untrusted chip is validated.

19. A validation system according to claim 11, where the time taken for the test function to return an indication the chip not validated is the same for all bad inputs, and the time taken to return an indication that the chip is validated is the same for all good inputs.

20. A validation system according to claim 11, where it is used to determine the physical presence of a valid authentication chip.